NUMBERS & ODDITIES

//////////////////////////// \\\\\\\\\\\\\\\\\\\\\\\\\\\\

- Editor: Ary Boender ***** e-mail: ary@luna.nl -
- Nickname on IRC channels #wun #monitor #numbers: Ary-B -

---------- Co-editors ----------

- Voice stations: Chris Smolinski <cps@access.digex.net> -
- Morse stations: Guy Denman <gdenman@mcmail.com> -
- Loggings: Jascha Ruesseler - -
- <ruessele@pc0401.Psychologie.Uni-Marburg.de> -

\\\\\\\\\\\\\\\\\\\\\\\\\\\\ ////////////////////////////

[- N&O #03 -]

Hello again! This month the first part of a series of crypto articles. Further the promised article about jamming and more station profiles.

PLEASE READ: Guy Denman told me that he is very disappointed because he gets no input from you at all. Unless more interest is shown, this might be his last contribution. I have the same experience; is it so hard to share your info and experience with your fellow dxers? Why don't YOU send us your logs, info, schedules, and questions? Especially info and logs regarding the Morse numbers stations are most welcome. The Morse scene is very much alive, but only few dxers seem to report them. Most of the logs so far, are voice station logs, which are of course also very welcome!

We like to extend our gratitude to those people who DID send their contributions. Thanks gang!

Oh, before I forget, please, mention your location (city, state and/or country) if you send us your logs.

Thanks for your co-operation and take care! -Ary-

CIPHERS AND SECURITY CHECKS

During the early days of WW2, routine and random security checks were inserted into all allied messages to verify that the sender was who he said he was, and to check whether or not he was transmitting under duress. Routine checks often comprised 'errors', such as the 3rd and 17th letter of a message misplaced by four places in the alphabet. Because the enemy quickly learned that these checks were inserted, the agents carried two codes, one to mislead the foe and one for messages to friends.

Because these checks weren't very safe, random checks were inserted into the messages. A three-letter code like 'wun', would be inserted at the begin and end of each message in normal situations. If the

sender was transmitting under duress, he would not insert the codes so that the receiver would know that he was in trouble. The code word at the beginning of the message would be disguised by advancing its letters by an agreed number of letters in the alphabet, while the same code placed at the end of the message, would be substituted by letters four places ahead in the alphabet. Example: code word = WUN, substituted by letters three places ahead in the alphabet. Result: 'ZXQ' (W=Z, U=X, N=Q) and substituted by letters four places ahead 'AYR'(W=A, U=Y, N=R). Two extra letters were added to camouflage the words as normal five-letter code words, e.g. ZXQ becomes AZXQW and AYR becomes BAYRP.

Only too often the security codes were forgotten by the field agent, or the home office thought that the agent had forgotten to add it, while in fact the agent did not add the code because he transmitted under duress. In short, this was not very safe and the allies phased this check out in 1942.

Other security checks included the use of phrases. These phrases were also used for short information exchanges. They often look funny, like 'the car needs a new engine', meaning that something was wrong, while 'there is no need for more coffee' could mean that everything was ok. Another one, noted on a British Army net: 'Zeppelins in the night sky' Reply: 'Pop them with a drawing pin'

The subject was discussed on Spooks a while ago. One of the comments came from Simon who says ''I read in one particular publication on the history of modern espionage that Radio Swan, the mysterious anti-Castro station sent "strange" messages on the day of the Bay of Pigs invasion in the form of coded sentences that made little sense, similar to the ones discussed in other postings.''

The other postings that Simon mentions include phrases like "Les sanglots longs des violons de l'automne percent mon coeur d'une langueur monotone" and "The water in the Seine is dirty". You can often hear sentences like these in WWII movies or TV-series. Some may be real, others a phantasy of the writer.

PLAYFAIR CODE: the Playfair code system had its origin in the UK. It was based on a phrase from a poem or song. The agent had to learn this line which was then transposed into blocks of five letters. The rest of the alphabet was used to fill the 5x5 letter square in an agreed order, the letters 'i' and 'j' counted as one. Double letters were omitted. Example: the phrase 'the numbers and oddities newsletter' would appear as:

T H E N U	The actual message was sent in bigrams
M B R S A	(= groups of two letters). The bigrams

```
   D O I W L                  were encoded by taking the two opposite
   P F K G C                  corners of the rectangle it formed in
   X Y Q V Z                  the square, eg DA becomes ML.
```

If both letters of the bigram are in the same line, then the next letters below are used; if both are in the same column, the next letters to the right are used, eg IW becomes KG and RI becomes SW.

The message 'spooks newsletter' in bigrams: SP OO KS NE WS LE TT ER and encoded: MG FF GR SR AL IU MM NS. After that the bigrams are grouped in five letter groups: MGFFG RSRAL IUMMN SZUQX. If the final group is too short, which is the case here, it is filled with dummy letters to complete it.

Because the system was too easy to break, it was replaced by other, more sophisticated systems in the early years of WWII.

ONE-TIME PADS: Many other systems, a.o. Delastelle -based on Fairplay- were used until the one-time pad was introduced. The one-time pad is one of the most successfull inventions of the spy-world. The system is unbreakable. It is easy to use and is in fact a very simple way of encryption, and very effective at the same time.

A one-time pad is a list of code groups, mostly five figure groups -but also other codes are used- printed on paper, silk handkerchiefs, or supplied on microfilm. Each group represents a certain phrase.

Example:
Guns and backup required - GB; Out of toiletpaper - OP. The two-letter codes should be repeated to avoid errors, eg GBGB and OPOP.

A more common way is the use of code groups, being a vocabulary of several hundreds words. The first five-digit group gives the index code; eg an incoming message starting with group 81114 would tell the agent that the decoding begins at page 81 line 114 of the code list. The next five-digit blocks are made up of three-letter codes, repre-senting the various phrases.

When an agent wants to send a message, he must use the codes for the relevant phrases. Example: the message 'I will cross the border tonight' has three relevant words, each with its own three-digit code.

```
   cross   = 321              The encrypted text would now read:
   border  = 551              321 551 873, or using five-digit groups:
   tonight = 873              32155 18730 (the '0' is a filler here).
```

Next is the transposition cycle. The agent would pick a page and line of the code list to encrypt the message itself, eg page 23 line 4. The

code line could look like this: 67554 23075 33687 18873 33109 99841

He now has to transpose the numbers of his message as follows. Subtract the lower number from the higher number without carrying across.

```
   67554 23075               The first group of the message would
   32155 18730               indicate the page and line: 23004
   ----- -----               followed by the encrypted message
   35499 15345               35499 15345
```

That's it for now. Next time we'll focus on other encryption techniques.

CW NUMBERS STATIONS by Guy Denman

Hi All,
For this month I will carry on with descriptions of some more of the families and what has been happening just lately.

* M8

Mode ICW. Uses Cut Numbers
T 0, A 1, N 2, D 3, U 4, W 5, R 6, I 7, G 8, M 9,
UAAMD MDUUA UAIAU R3   UAAMDx5 = = = 150f Cut
After first message sends AR AR AR MDUUAx5 = = = 150f Cut same after second message
Ends AR AR AR SK SK SK

This is now the usual format, at least 2 others exist.

The station is usually active in the mornings up to 1100. I have heard it at 0600, but as I do not get up early nowadays, not sure how much earlier it is on. I have seen reports from the USA of it being on from 0000 onwards. I am still not sure if the ones we can hear in the UK are being transmitted from Cuba. They are quite often S9 signals, which sound too strong for that distance. Logged an unusual one recently with the last figure of the ID being 4. They are normally 1, 2 or 3.

Some frequencies in use are: 6287 6787 6797 6825 6933 7580

-o-o-o-o-o-o-o-o-o-o-

* M10

Always uses ICW. This station uses a slightly different format of 2 figure decode key. The call up usually starts with 555 but they have been known to use other triplets, 111 222 333 444 777 and 888. These

are used on special broadcasts. They have also be known to use up to a 4/5 figure random ID, but only very rarely. Transmission times and frequencies are changed quite often, although they use a set of frequencies to choose from. Sometimes they use 2 frequencies but not always. Regular schedules all use 2 parallel frequencies.

The speed the message is sent is variable, usually the later message is sent at a faster speed. Call and first message 17 WPM later messages up to 25 WPM.

Call	Preamble	Message	Ending
555x3 571x3 46 (R5)	571x3 75 75 46 46 = =	46x5F = =	75 75 46 46 000

They can have up to 4 IDs in the call, in this case the call would be

555x3 571x3 46 275x3 25 049x3 16 435x3 41 (R5)

Then the preamble would be the same, message the same but the ending misses off the 000 and carries on to the next call which would be 275.

There is a regular sked with these 4 IDs on Saturday, Sunday, Monday and Wednesday at 1645. frequency 4485//5028. Same messages repeated for 4 days.

The message can also sometimes be split into 2 parts with a different decode key for each part, but in this case the call gives the total amount of groups in the message.

Frequencies that have been used are:

3385	3834	4029	4305	4485	4541	4573	4775
4834	4882	5007	5025	5040	5060	5085	5155
5276	5290	5301	5295	4525	5471	5503	5521
5554	5702	5737	5760	5860	6204	6758	6780
6801	6835	6943	7380	7404	7475	7845	8111
8175	8190	9164	9369	9386	9455	9971	10582
10922	11415	121??	125??	13405	14977	14650	14562

Some skeds active at present as of 9 January 1998

Sunday	1645 3385//	1810 4029//	1920 5471//
Monday	0820 8190//9164	1645 3385//	1920 5471//
Wednesday	1645 3385//4485		
Thursday	1810 4029//		
Saturday	1645 3385//		

Schedules are Monthly, twice Monthly, or weekly. always repeated within the same week. Special schedules (irregular) may be daily. Another slightly different format has been logged recently, the station comes on at 2000 on 3824. It is not regular so may be heard

any day of the week.

Format is:
Call 111x3 55013x3 30x3 for 5 minutes
55013x3 02 02 30 30 = = 30x5F {Always 30 groups} = = 02 02 30 30
does not end with 3 zeros as the normal M10

It is sometimes hand sent, when all the rest of M10 are always auto sent. Was on Friday 12 June to ID 12127

-o-o-o-o-o-o-o-o-o-o-

* M12

Mode Usually ICW but has been known to use MCW. The call is sent fairly slowly at about 15 WPM but the preamble and messages are usually sent at 30 WPM, single 5 figure groups, although slower and faster speeds have been used. They are constantly changing frequencies and transmission times so it is not worth listing them.This is another station that has been noted using the same frequencies and IDs as in 1997. The message is sometimes repeated on a further two frequencies. If the message is sent on the hour then there will be the same message sent at Hour+20 Hour+40, Hour+25 Hour+45, or Hour+30 Hour+50, this depends on length of message and speed sent. Can be found on at any time.

Call	Preamble	Message	Ending
749 749 749 000 R5		No Message	
749 749 749 1 R5	1573 143 1573 143	143x5f	Pause 000 000

The figure 1 after 749 indicates number of messages,2 messages are very rare. There is one message that keeps on being sent, that has been sent for some considerable time. I first logged it in October 1996 but I know it has been logged before this, usually sent to an ID starting with the figure 3. At present being sent to 314.

The preamble is 792 66 792 66 and the message is always the same. They are still coming on the same frequency as used last year with some variations. Last year on a Friday there was one on at 1600 on 12132 which repeated at 1700 on the same frequency. It is on again this year at 1600 on 12132 but now is the usual format, coming on at 1620 on 13544 and 1640 on 14728. ID was the same 963.

-o-o-o-o-o-o-o-o-o-o-

Activity is still high this last month. M29 had a particularly busy day on Thursday 11 June. I heard it six times sending messages, also G4 was on at the same time.

M3 is still coming on the same frequencies as last year, and in some cases sending the same messages. It was on Friday 12 June at

    0800 on 5365 041/00
    0830 on 5624 017/00
    0900 on 5050 012/00

and 0930 on 6430 552/00 an exact repeat of 1997.

M53 came on friday 5 June at 2000 with one of its very rare double messages, call was 747.750.016 Message to 750 was 30 groups, followed by a message of 33 groups to 016.

Thats all for this Month, if anyone finds the morse station information useful I would appreciate an e-mail. If anyone requires further information the same applies.

73, Guy

WORLDWIDE JAM SESSION

Here is the promised jamming article. The article gives some info about jamming in general and the various types of jammers. In next month's column I will publish the frequencies and findings of the few readers who were so kind to send me their jammer-logs and comments.

-o-o-o-o-o-o-o-o-o-o-o-

Everyone must have heard them, those odd sounding signals. Pulse jammers, and bubble jammers with their typical 'woo woo woo' sound, are the most common types of jammers on SW. The amount of jammers is amazing in the 4, 5 and 6 MHz bands, especially in the evening between 1900-2100 UTC and at night between 0200-0400 UTC, equalling the late evening and early morning in the Middle and Far East, where most of the jamming nowadays originates.
Top of the list of suspects are Iran, Iraq and Cuba. The USA may be responsible for the jamming of Iraqi and Iran based stations. Possibly using jammers in EW-aircraft or vessels. Cuba jams Radio Miami, Radio Marti, WRMI, and stations which relay La Voz de la Fundacion (WHRI, maybe some others). Radio Free Asia reported jamming of its Vietnamese and Chinese services by possibly China, North Korea or Vietnam.

Aeronautical, maritime and SAR stations suffer from these activities. Tony Orr, WUN's aeronautical editor wrote in his column: ''Many of you have by now either heard or heard about the troubles with jammers in the 5 MHz range of frequencies lately. These jammers, targeting a certain clandestine station broadcasting from the Middle East, are literally all over the band, causing the aeronautical ground stations operating there

to scramble for new frequencies to use in lieu of their regular 5 MHz homes. Especially hard hit was Gander Radio on 5649 kHz, which has seen fit to move down to 4675 kHz for it's operations on NAT-C.''

Tony is right, I heard it myself. Recently Dutch Coast Guard aircraft had to change frequency because of this problem. SAR frequency 5680 kHz is also a victim. SAR monitor Alan Gale from the UK sent me the following comments:
''The interefrence on 5680 kHz first appeared around the 2 August 1997. It fades in here in the UK around 1600 UTC every evening. The AM station comes on air, and quickly gets jumped on by a 'Bubble Jammer'. After a while the station stops broadcasting and the jammer also stops, but then seconds after the broadcast restarts again the jammer also returns.

The clandestine station which was heard on 5680 kHz in the clear before the jammer caught up with it had a YL presenter. Shortly afterwards what sounded to be the same presenter was heard on 5670, 5660 and 5630 kHz. The pattern seemed to be transmit on one channel until the jammer commenced, and then QSY to another channel on steps a multiple of 10 kHz away. As soon as the jammer caught up with them they stopped transmitting, though in many cases a blank carrier remained on channel and the jamming continued. The jammer only ceased when the carrier appeared to be switched off.

No Station IDs were heard, but the words 'Iran' and 'Rafsanjani' were heard on the station on 5680 with the YL presenter. On another occasion the name 'Khomeni' was heard several times, and if as seems likely, this is 'The Voice of the Mohajed' operating from the Iraqi border into Iran this would make sense. There may well be a set pattern as to which channel the station changes to when the jamming commences, it would be difficult for listeners if there wasn't. A regular pattern would make life easier for the jammers though, so a further study of this might well prove interesting.''

* How it all started

Jamming was first used by the Germans during World War 1. In the early 1920s, competing broadcasters in the United States jammed rival radio programs. During the 1930s, jamming became a political weapon. World War II demonstrated that a jamming network operating against military circuits, was a potent wartime weapon.

"Knickebein" was an early guided weapon system. The Germans invented this system and used it in WWII. It used two beams; one transmitted from Kleve for guidance, and a second cross-beam from Bredstedt. The bombers followed the first beam until it intersected the second, directly over the target, and dropped their bombs.

Documents retrieved from downed German bombers showed that the beams operated on a frequency of 30 MHz. In those days the only receiver that was capable of detecting the beams was the Hallicrafters S-27. Fitted to a search aircraft, the beam was detected. The Germans made this work easier by testing their system over England instead of Germany.

Knickebein was called "headache" by the British, and jammers dubbed "aspirins" were developed. Soon German bombing accuracy diminished due to the interference of the British jammers.

The War's end saw jamming continued but on an even larger scale, especially with the advent of the Cold War. Stalin decided in 1948 to launch massive jamming campaigns against the West. At first, the commitment was made using a dozen jammers operating against Russian-language broadcasts of the Voice of America. By 1956 about 3,000 Soviet block jammers were operating against Western broadcasts in all languages. Their jamming system was administered by a secret department in the Ministry of Communications, privately known as the Krestyaninova Section. It was named after Natalia Krestyanoniva who ran the department for more than twenty-five years.

* Introduction to Jamming

The purpose of all jamming is to interfere with the enemy's effective use of the electromagnetic spectrum. Use of the spectrum involves the transmission of information from one point to another. This information can take the form of voice or non-voice (e.g., video or digital format) communications, command signals to control remotely located assets, data returned from remotely located equipment or the location and motion of friendly or enemy assets (land, sea or air).

Type of Jamming	Purpose
Communications Jamming	Interferes with enemy ability to pass information over a communications link.
Radar Jamming	Causes radar to fail to acquire target, to stop tracking target or to output false information.
Cover Jamming	Reduces the quality of the desired signal so it cannot be properly processed or so that the information it carries cannot be recovered.
Deceptive Jamming	Causes a radar to improperly process its return signal to indicate an incorrect range or angle to the target.
Decoy	Looks more like a target than the target does.

Causes a guided weapon to attack the decoy rather than its intended target.

For many years, jamming has been called electromagnetic countermeasures (ECM), but it is now referred to in most literature as electronic attack (EA). EA also includes the use of high levels of radiated power or directed energy to physically damage enemy assets. Jamming is sometimes called "soft kill" because it temporarily makes an enemy asset ineffective but does not destroy it.

The basic technique of jamming is to place an interfering signal into an enemy receiver along with the desired signal. Jamming becomes effective when the interfering signal in the receiver is strong enough to prevent the enemy from recovering the required information from the desired signal, either because the information content in the desired signal is overwhelmed by the power of the jamming signal or because the combined signals (desired and jamming) have characteristics that prevent a processor from properly extracting or using the desired information.

Communications jamming (COMJAM) is the jamming of communications signals. This is normally considered the jamming of tactical HF, VHF and UHF signals using noise-modulated cover jamming, but it can also mean the jamming of point-to-point microwave communications links or command and data links to and from remote assets.

The effectiveness of a jammer is calculable only in the context of the enemy receiver that it jams. The most common way to describe that effectiveness is in terms of the ratio of the effective jammer power (i.e. the jamming signal power that gets into the heart and soul of the receiver) to the signal power (that the receiver really wants to receive). This is called the "jamming to signal ratio," or the "J-to-S ratio," or simply the "J/S."

Jamming signals are, by their nature, one-way transmissions. In general, the performance of the jamming signal is the same whether its target is a communications receiver or a radar receiver. Its acceptance by the receiver differs from that of the desired signal in two ways.

- First, unless the receiver has an omnidirectional antenna, the antenna gain will vary as a function of the azimuth or elevation from which the antenna receives signals. Thus, the jamming and the desired signal will experience different receiving antenna gains unless they arrive from the same direction.
- Second, jamming signals must often be much wider in frequency than the signals they are jamming because the desired signal's exact frequency cannot be measured or predicted. In predicting the J/S, it is important to count only the part of the jamming signal power that falls within the receiver's operating bandwidth.

Every type of receiver must have an adequate signal-to-noise ratio (SNR) in order to properly process the signals it is designed to receive. The SNR is the power ratio of the desired signal to the noise power in the receiver's bandwidth. The received desired-signal power is a function of the transmitter power, the length of the transmission path, the operating frequency and (for radars) the radar cross section (RCS) of the target. Cover jamming injects additional noise into the receiver, which has the same effect as increasing the transmission-path length or decreasing the RCS of a radar's target.

When the jamming noise is significantly higher than the receiver's thermal noise, we speak of the jamming-to-signal (J/S) ratio rather than the SNR, but the effect on signal reception and processing is the same. If cover jamming is increased gradually, the operator or the automatic processing circuitry following the receiver may never become aware that jamming is present - only that the "SNR" is becoming extremely low.

The required RCS depends on the nature of the received signal and the way it is processed to extract its information. For voice communications, the SNR will depend on the skill of the speaker and the listener and the nature of the messages being passed. Effective communication ceases when the SNR rises to the point at which no information can be received. For digital signals, inadequate SNR causes bit errors and communication ceases when the bit error rate is too high to pass messages.

If frequency hopping is employed in either radar or communications applications, the frequency band accepted by the receiver is a "moving target" When other types of spread-spectrum techniques are used, the signal is spread over a wide frequency range that the receiver can reverse to achieve the sensitivity appropriate to the signal before it was spread. The problem for the jammer is that to be effective, it must spread its available power over the entire frequency that the receiver might be receiving - over all the angular space that might contain the receiving antenna - during all of the time that the receiver might be accepting signal energy. Still, it is only the amount of power that gets through all of the receiver's defenses, that contributes to J/S. Since a jammer's transmitter power is directly related to its size, weight, prime power availability and cost, the answer is seldom just to increase the jammer output power until there is enough effective jammer power.
The more the jammer knows about the operation of the receiver, the more narrowly it can focus its jamming power to what the receiver will notice. Jammer energy-focusing is called "power management," and it can only be as good as the information available about the jammed receiver. The bottom line is that the jammer can concentrate its power where it will do the most good.

* The great carriers hunt

Many dxers -especially the 'spook hunters-, often report carriers on many frequencies between 4 and 6 MHz. Sometimes a station pops up after a while, but most of the times nothing happens. At least that's what you think. Although I have no solid proof, I am pretty sure that these carriers have a purpose, namely to attract jammers. When the jammers are busy jamming the carriers, the station itself can broadcast without being jammed.

A few examples:
The 'chase': 5721 17.03 jammer, stopped at 17.03; jumped to 5680 at 17.05 because there was an carrier. Both carrier and jammer stopped at 17.06. The jammer jumped from 5680 to 5729 and stopped after one minute. Then to 5768 at 17.07 and stayed there also for one minute. Back again to 5729 where it was active for quite a while.

Another one: 5660 17.45 UTC a Clandestine? stn with a marching song and a male voice in unid language came on. Its signal was good. About 30-40 seconds later, the jammer on 5658 jumped to 5660 kHz. 10 seconds later two other jammers joined in, all power houses. Very loud. The station often changed frequency, hopping up and down the dial with no obvious "strategy" in 10, 20 or 30 kHz steps. It was chased by 3 jammers. It took the jammers not much time to catch up with the station.

''Is someone listening to all these frequencies so that he can switch on the jamming device at the right moment?'', you may ask. No, not really. But it's close..... This is how it works:

o HF JAMMING SYSTEMS
often have automatic frequency control tracking capabilities for signal analysis, so that you can select a mode that has to be jammed (eg CW or voice). A look-through feature suspends jamming when a target's trans-mission has stopped, immediately directing the system to other freqs selected for jamming. This automatically means that the jamming of SAR frequency 5680 kHz is either intentionally or they just don't care, as virtually all modern systems work with databases filled with target frequencies. You can include or exclude frequencies very easily, so they probably just don't care who they are jamming.

o VHF JAMMING
works in slightly different way: a computer allows the Jam-System to constantly monitor the frequency range and to respond instantly to changes in the electro-magnetic environment. Then it starts its jamming activities.

* Field Manual 24-33

The various types of jamming signals are described in the US Army

Field Manual 24-33 chapter 3. This is an exact quote of the relevant parts of the text, hence the 'we', 'us' and 'our' expressions :-)

o Types of Jamming Signals
Jamming is an effective way for the enemy to disrupt our command, control, and communications on the battlefield. All the enemy needs to jam us is a transmitter tuned to our frequency with enough power to override friendly signals at our receivers. Jammers operate against receivers--not transmitters. There are two modes of jamming: spot and barrage. Spot jamming is concentrated power directed toward one channel or frequency.
Barrage jamming is power spread over several frequencies or channels at the same time. Jamming can be difficult, if not impossible to detect. For this reason, we must always be aware of the possibility of jamming and be able to recognize it. The two types of jamming most commonly encountered are obvious and subtle jamming.

A) Obvious jamming
This is normally very simple to detect. The more commonly used jamming signals of this type are described below. Do not try to memorize them; just be aware that these and others exist. When experiencing a jamming incident, it is more important to recognize and overcome the incident than to identify it formally.

* Random noise
This is synthetic radio noise. It is random in amplitude and frequency. It is similar to normal background noise and can be used to degrade all types of signals. Operators often mistake it for receiver or atmospheric noise and fail to take appropriate ECCM actions.

(note: this one sounds like a sudden increase in athmospheric noise. A variation of this type transmits noise bursts. -Ary-)

* Stepped tones
These are tones transmitted in increasing and decreasing pitch. They resemble the sound of bagpipes. Stepped tones are normally used against single-channel AM or FM voice circuits.

* Spark
The spark signal is easily produced and is one of the most effective for jamming. Bursts are of short duration and high intensity. They are repeated at a rapid rate. This signal is effective in disrupting all types of radio communications.

* Gulls
The gull signal is generated by a quick rise and slow fall of a variable radio frequency and is similar to the cry of a sea gull. It produces a nuisance effect and is very effective against voice radio

communications.

* Random pulse
In this type of interference, pulses of varying amplitude, duration, and rate are generated and transmitted. They are used to disrupt tele-typewriter, radar, and all types of data transmission systems.

(note: this pulse-keyed CW signal sounds like a power drill. -Ary-)

* Wobbler
The wobbler signal is a single frequency which is modulated by a low and slowly varying tone. The result is a howling sound that causes a nuisance effect on voice radio communications.

(note: this type is also known as 'warble' or 'bubble' jammer. It sounds like 'woo woo woo woo' -Ary-)

* Recorded sounds
Any audible sound, especially of a variable nature, can be used to distract radio operators and disrupt communications. Music, screams, applause, whistles, machinery noise, and laughter are examples.

(note: the 'backwards music station' (XM) and 'the workshop' (XW) are good examples, also the one that Simon calls the "Reverberator" which, as the name suggests, sounds like endless reverberation - similar to the sound of a crowded room. -Ary-)

* Preamble jamming
This type of jamming occurs when a tone resembling the synchronization preamble of the speech security equipment is broadcast over the operating frequency of secure radio sets. Preamble jamming results in all radios being locked in the receive mode. It is especially effective when employed against radio nets using speech security devices.

(Additional jamming signals, not mentioned in FM24-33 are:
* Carrier-sweep
This one sounds like an automobile engine at high-speed.

* Grunting
Produced by modulating an AM transmitter with a very low audio frequency varying at a random rate. Sounds exactly like it is named)

B) Subtle jamming
Subtle jamming is not obvious; no sound is heard from our receivers. They cannot receive an incoming friendly signal, even though everything appears normal to the radio operator. Subtle jamming takes advantage of design features of the AN/PRC-77 and AN/VRC-12 series radios. In order to activate the receiver of an AN/PRC-77 in the SQUELCH mode or an

AN/VRC-12 series radio in the NEW SQUELCH ON mode, a 150-hertz tone must be transmitted to them along with the carrier signal. In addition to this squelch feature, the AN/PRC-77 and AN/VRC-12 series radio receivers lock onto the strongest carrier signal received and eliminate the reception of all other signals. For example, if we have an AN/PRC-77 in the SQUELCH mode and an AN/VRC-12 series radio in the NEW SQUELCH ON mode and they receive a jamming signal without the 150-hertz tone, the receivers of these radios will not be activated by any signal as long as the jamming signal is stronger than any other signal being received. In effect, the threat jammers block out these radios' ability to receive a friendly transmission without the operator being aware it is happening. This is called squelch capture and is a subtle jamming technique. The radio operator can readily detect jamming in all other function control modes and the other modes must be checked. Often, we assume that our radios are malfunctioning instead of recognizing subtle jamming for what it is.

o Recognizing Jamming
Radio operators must be able to recognize jamming. Again, this is not always an easy task. Threat jammers may employ obvious or subtle jamming techniques. Also, interference may be caused by sources having nothing to do with enemy jamming. Interference may be caused by the following:

- Unintentionally by other radios (friendly and enemy).
- Other electronic or electric/electromechanical equipment.
- Atmospheric conditions.
- Malfunction of the radio.
- A combination of any of the above.

Internal or external interference.
The two sources of interference are internal and external. If the interference or suspected jamming can be eliminated or substantially reduced by grounding the radio equipment or disconnecting the receiver antenna, the source of the disturbance is most likely external to the radio. If the interference or suspected jamming remains after grounding or disconnecting the antenna, the disturbance is most likely internal and is caused by a malfunction of the radio. Maintenance personnel should be contacted to repair it. External interference must be checked further for enemy jamming or unintentional interference.

Jamming or unintentional interference.
Unintentional interference may be caused by other radios, some other type of electronic or electric/electromechanical equipment, or atmospheric conditions. The battlefield is so crowded with radios and other electronic equipment that some unintentional interference is virtually unavoidable. Also, the static electricity produced by atmospheric conditions can negatively affect radio communications. Unintentional interference normally travels only a short distance, and a search of the immediate area may reveal the source of this type of interference.

Moving the receiving antenna for short distances may cause noticeable variations in the strength of the interfering signal. These variations normally indicate unintentional interference. Conversely, little or no variation normally indicates enemy jamming.

The enemy can use two types of jamming signals: powerful unmodulated or noise-modulated signals. Unmodulated jamming signals are characterized by a lack of noise. Noise-modulated jamming signals are characterized by obvious interference noises.

o Overcome jamming
Adjust the receiver. When jamming is experienced, we should always check to ensure the receiver is tuned as precisely as possible to the desired incoming signal. A slight readjustment of the receiver may provide an improved signal-to-jamming ratio. Depending on the radio being used, some of these methods are:

Adjust the beat frequency oscillator (BFO).
Adjust the bandwidth.
Adjust the gain or volume control.
Fine tune the frequency.

Adjust or change the antenna. Antenna adjustments can appreciably improve the signal-to-jamming ratio. When jamming is experienced, the radio operator should ensure the antenna is optimally adjusted to receive the desired incoming signal. Depending on the antenna being used, some of these methods are:

Reorient the antenna.
Change the antenna polarization. (Must be done by all stations)
Install an antenna with a longer range.

Relocate the antenna. Frequently, the signal-to-jamming ratio may be improved by relocating the antenna and associated radio set affected by the jamming or unidentified interference. This may mean moving a few meters or several hundred meters. It is best to relocate the antenna and associated radio set so that there is a terrain feature between them and any suspected enemy jamming location.

-o-o-o-o-o-o-o-o-o-o-o-

Sources:
Anthony Uminn, Paige Chia, William Kangas ('Jamming Radio Signals', 1997)
'Codebreaking and Secret Weapons in World War II' by Bill Momsen
JED - Journal of Electric Defense
US Army Field Manual 24-33 chapter 3
US Army Field Manual 34

Special thanks to the following dxers for their logs and comments: Tony Orr, Alan Gale, Iron Eagle, Markus Buttinger, Day Watson, Alec Muffett, Clarence Thompson, John Maky, Roger Preston, Simon Denneen, and various anonymous dxers.

****
Numbers + Oddities Logs column
Jascha Ruesseler
Ruessele@pc0401.psychologie.uni-marburg.de
****
Hi, folks, her we go again..
Our log format is as follows:

FREQ c/s Station (Enigma Code) Time (date) Mode (baud) Remarks (Initials)

Example:
10426 Lincolnshire Poacher (E3) 1540 (April 13) USB ongoing msg (JR)

The logs in this column are taken from the spooks mailing list. I also include some logs from the wun-list which are not cross-posted to spooks. If you want to remain anonymous, you can sent your logs to me or Ary.

2626 Mossad (E10) 1731 (June 7) USB unable to make out id but passed 2 msgs (SD)
3927 atencion stn (V2) 0100 (May 31) (BR)
4016 cut no's CW (M8) 0300 (June 1) (BR)
4028 ?? cut no's (M8) 0300 (June 9) CW ANRMA MMGNA NNGTA (BR)
4029 Spanish Lady 0530 (June 5) AM YL/SS 5F groups. Off at 0545 UTC with "FINAL"x3.(JM)
4120 //4450 Reverberator 1004 (May 27) AM in progress (SD)
4165 ?: Mossad, ISR 22.18 (May 21) USB MIW2 transmission (AB)
4174 Spanish Lady (V2) 1002 (May 27) USB in progress (SD)
4479 Atencion stn (V2) 0300 (May 26) (BR)
4479 atencion stn (V2) 0300 (June 2) (BR)
4479 atencion stn (V2) 0300 (June 10) AM (BR)
4506 cut no's CW (M8) 0100 (May 28) (BR)
4506 cut no's CW (M8) 0300 (June 2) (BR)
4625 The Buzzer (S28) 1453 (June 11) USB idle mode (SD)
4665 ?: Mossad, ISR 22.20 (May 21) USB KPA2 transmission (AB)
4506 cut no's stn (M8) 0300 (June 10) CW (BR)
4506 cut no's stn (M8) 0100 (June 11) CW very weak & noisy condx (BR)
4973 RR/F (S21) 1742 (May 28) AM 973R4 798 798 41 41 (GD2)
5116 cut no's stn (M8) 0200 (June 12) CW (BR)
5180 Cherta (S12) 2100 (June 3) 671/00 Not sure of first figure of

ID (GD2)
5230 Mossad (E10) 1815 (June 7) USB id MIW2 (SD)
5340 English (G2) 0757 (May 28) AM 58955 01331 71226 (GD2)
5419 cut no's CW (M8) 0200 (June 1) (BR) 5416 cut no's CW (M8) 0300 (June 2) (BR)
5416 cut no's stn (M8) 0300 (June 10) CW (BR)
5435 Mossad (E10) 1802 (June 7) USB id ART with 2 msg grps 14 & 93 (SD)
5435 Mossad (E10) 1502 (June 14) USB id ART2 (SD)
5629 Mossad (E10) 1816 (June 7) USB id KPA2 (SD)
5630 Three Note Oddity (sorry, i deleted the time-ed.) (June 7) USB msg. (HFD)
5688 Babbler 1325 (May 24) USB SP W test counts. (ANUS)
5637 Babbler 2242 (May 23) USB idle (ANUS)
5730 Three Note Oddity 2005 (June 7) USB Msg.: 32147 65458 21002 95458 32125 45214 05658 78547 66655 22147 32125 45214 84547 05458 32125 44520 33321 85457 33258 65452 45214 55547 32125 00087 32125 Note the "32147" on 1 and "32125" 5, 11, 15, and 25 (HFD)
5758 cut no's CW (M8) 0300 (June 4) (BR)
5758 cut no's stn (M8) 0200 (June 10) CW with MTWTN GDGAN ATUGN (BR)
5800 atencion stn (V2) 0300 (June 1) (BR)
6797 atencion stn (V2) 0200 (June 1) (BR)
6825 cut no's CW (M8) 1200 (May 28) (BR)
6825 ?? cut no's (M8) 0200 (June 9) CW (BR)
6825 cut no's stn (M8) 1200 (June 11) CW (BR)
6826 atencion stn (V2) 0300 (June 1) (BR)
6826 atencion stn (V2) 0300 (June 2) (BR)
6826 atencion stn (V2) 0300 (June 10) AM (BR) 6855 atencion stn (V2) 0300 (June 1) (BR)
6867 Russian man (?) 0200 (June 10) msg 538 then 5fig x 2 (BR)
6868 Bored Man 1406 (May 24) USB "R290" msg // 4106. (ANUS)
6982 ?? cut no's (M8) 1200 (June 8) CW (BR) 6982 cut no's stn (M8) 1200 (June 15) CW (BR)
6983 atencion stn (V2) 0200 (May 29) strong carrier, weak audio (BR)
6983 atencion stn (V2) 0200 (June 12) AM (BR)
6985 Spanish Lady 0204 (June 11) AM SS/YL/5FG Ended with three "hello?"s (JL)
7250 English (G2) 0957 (May 28) AM Repeat of above /GD2)
7337 ?: Lincolnshire Poacher, CYP 22.00 (May 21) USB Id 28065. //9251 //12603 kHz (AB)
7540 Mossad (E10) 1532 (June 14) USB id JSR2
7583 atencion stn (V2) 0200 (June 10) AM (BR)
7726 Spanish Lady (V2) 0538 (June 3) AM in progress (SD)
7888 ?? cut no's (M8) 0100 (June 9) CW RIRTA RWMWD GDGAA (BR)
8188 English (G2) 0957 (May 28) AM Repeat of above (GD2)
8320 // 12056 // 13866 E4 1200 USB 78640 (7) beeps 42200 5ngs. All frqs were good today.(CT)
8320 // 12056 (E4) 1200 (June 3) usb 03191 5ngs.(CT)

noticed parkhall voice scrambling on 8320 usb today (June 3) (CT)
8320 s7dB // 12056 s1dB // 13866 s1dB Cherry Ripe (E4) 1200 (June 8) usb 94275 5ngs 86273 86273.(CT)
8320 // 12056 // 13866 e4 Cherry Ripe 1200 (June 12) usb 33437 5ngs good signals this am local.(CT)
8320 s7dB // 13866 s2dB // 12056 s3dB cherry ripe (E4) 1200 (June 17) usb 58820 5ngs 05104.(CT)
8983 Backwards Music Station (XM) 1738 (June 7) USB in progress (SD)
9130 Mossad (E10) 0525 (June 3) USB id EZI2 (SD)
9218 X6 Polytone Station (tent) 0606 (May 27) (SD)
9218 High Pitched Polytone (XPH) 0605 (May 27) AM in progress (SD)
9238 Spanish Lady (V2) 0604 (May 27) AM in progress (SD)
9238 Spanish Lady (V2) 0600 (June 3) AM unable to make out id (SD)
9260 atencion stn (V2) 0200 (June 10) AM (BR)
9263 Cherry Ripe (E4) 1115 (June 3) usb 5 ngs missed callup.(CT)
9263 // 13688 // 14469 Cherry Ripe (E4) 1100 (June 15) usb 94349 5ngs(CT)
9326 Russian Man (S6) 0528 (June 4) USB in progress (SD)
9394 XPH - High Pitch Polytone Station 0602 (June 5) AM SINPO55545 Off at 0604z (ABe)
10223 count stn (E5) 1200 (June 10) USB msg 869 count 215 (BR)
10223 count stn (E5) 1200 (May 26) with msg 829 count 215 (BR)
10223 count stn (E5) 1200 (June 2) with msg 869 count 215 (BR)
10328 BPA FAPSI (M42) 1530 (June 6) rpt of above (BR)
10529 count stn (E5) 1300 (June 5) with msg 117 count 215 (BR)
10529 TCS 1300 (May 16) AM "CIA" station (JL)
10566 cut no's CW (M8) 1300 (June 5) (BR)
10597 Count stn (E5) 1500 (June 5) USB msg 194 count 126 (BR)
10711 Spanish Man (V7) 0600 (May 28) AM 725x3 000 Null message Repeats same message as sent by M45 at 1702 on 5474 (GD2)
10858 cut no's CW (M8) 1200 (May26) with RGRND UWMID DDWGD (BR)
10858 cut no's CW (M8) 1200 (May 28) (BR)
10858 ?? cut no's (M8) 1200 (June 9) CW (BR)
10858 cut no's stn (M8) 1200 (June 11) CW (BR)
11149 V7 - Spanish Man 0600 (June 9) AM ss/om/frequency id-118/message-1/id key-1723/gc-50/5fg SINPO 55545 off at 0610z with 000 000. Tx moved imediately to 12149 kHz. (ABe)
11149 Spanish Man (V7) 0600 (June 11) ss/om/frequency id-118/ call-'000'/no traffic SINPO 55555 off at 0605z. Tx moved after one minute to 12149. (ABe)
11149 Spanish Man (V7) 0600 (June 16) AM ss/om/frequency id-118/message-1/id key-810/gc-37/5fg SINPO 55444 off at 0609z with 000 000. Tx moved to 12149 kHz within 1 minute. Tx went off momentarily during first few 5fg. (ABe)
11149 Spanish Man 0600 (June 18) AM ss/om/frequency id-118/message-1/id key-810/gc-37/5fg

SINPO 55555 off at 0609z with 000 000. Tx moved to 12149 kHz at 0611z. Heavy Buzz on Tx. (ABe)

11461 cut no's CW (M8) 0200 (June 1) (BR)

11494 XPH - High Pitch Polytone Station 0621 (June 5) AM SINPO55545 Off at 0624z (ABe)

11570 // 13866 // 7484(qrn digi) Cherry Ripe (E4) 1300 (June 12) 63696 5ngs.(CT)

11637 GMN FAPSI (M42) 0045 (June 11) RTTY (75/425) with 46's - no tfc (BR) 12056 ?: Cherry Ripe, ? 22.00 (May 21) USB Id 35624. //9263 //15624 kHz (AB)

12149 V7 - Spanish Man 0620 (June 9) ss/om/frequency id-118/ message-1/id key-1723/gc-50/5fg SINPO 55444 off at 0630z with 000 000. Tx moved imediately to 13849 kHz. (ABe)

12149 Spanish Man (V7) 0610 (June 11) ss/om/frequency id-118/ call-'000'/no traffic SINPO 55545 off at 0616z. Tx off imediately. (ABe)

12149 Spanish Man (V7) 0620 (June 16) AM ss/om/frequency id-118/message-1/id key-810/gc-37/5fg SINPO 55555 off at 0629z with 000 000. Tx moved to 13849 kHz at 0630z. (ABe)

12200 Spanish Lady 0208 (June 8) AM SS/YL/5FG (JL)

12215 ?? cut no's (M8) 0100 (June 9) CW TWRTA TATDA TGNMA (BR)

13452 JMS FAPSI RTTY (M42) 2245 (May 25) with 4/671 msgs (BR)

13452 JMS FAPSI RTTY (M42) 2230 (June 2) with 2/180 msgs (BR)

13452 JMS FAPSI (M42) 2239Z (June 12) RTTY (75/425) rpt of above (BR)

13380 UMK:FAPSI 0010z (June 2) RTTY 75/1000 w/UMK QTC 46s w/one msg : 11144 00155 24018 01064 01659 w/5LGs, unusual shift for this net (ML)

13849 Spanish Man (V7) 0640 (June 16) ss/om/frequency id-118/message-1/id key-810/gc-37/5fg SINPO 55545 off at 0649z with 000 000. (ABe)

13906 count stn (E5) 1200 (June 10) USB msg 222 count 215 (BR)

13394 XPH - High Pitch Polytone Station 0640 (June 5) AM SINPO55555 Off at 0644 (ABe)

13556 HZW FAPSI RTTY (M42) 2012 (May 30) with 2/492 msgs (BR)

13849 V7 - Spanish Man 0640 (June 9) ss/om/frequency id-118/ message-1/id key-1723/gc-50/5fg SINPO 55444 off at 0650z with 000 000. (ABe)

13906 count stn (E5)1200 (June 2) with msg 222 count 215 (BR)

14000 ?: Numbers station E15, ? 17.00 (May 20) USB id Frank Young Peter (AB)

14434 KRN FAPSI (M42) 1744 (June 5) rpt of above (BR)

14487 ?: Lincolnshire Poacher, CYP 17.00 (May 20) USB id 18647 (AB)

14731 BPA FAPSI (M42) 1515 (June 6) RTTY/75 msgs 2/747 (BR)

14843 JMS FAPSI RTTY (M42) 2230 (May 25) with 4/671 msgs (BR)

14843 JMS FAPSI RTTY (M42) 2230 (June 2) with 2/180 msgs (BR)

14843 JMS FAPSI (M42) 2230 (June 8) RTTY/75 msgs 4/1039 (BR)

14843 JMS FAPSI (M42) 2230 (June 9) RTTY/75 msgs 5/989 (BR)

14843 JMS FAPSI (M42) 2230 (June 12)   RTTY (75/425) with 1/207 msg (BR)
14843 JMS FAPSI (M42) 2230 (June 15)   RTTY (75/425) with 2/210
       msgs (BR)
14930 Spanish Lady 0109 (June 6) AM SS/YL/5FG (JL)
15478 // 16050 count stn (V5) 0100 (May 29) with msg 902 (BR)
15478 //16050 count stn (V5) 0100 (June 10) USB msg 902 (BR)
15624 //19884//21866 Cherry Ripe (E4) 0103Z (June 11) USB id 94275 (SD)
15682 Linconshire Poacher E4 1408 (June 5) 321-24 very weak here. (EB)
16218 HZW FAPSI RTTY (M42) 2000 (May 30) with 2/492 msgs (BR)
16218 YBU FAPSI RTTY (M42) 1400 (June 4) with 1/75 msg (BR)
16218 YBU FAPSI RTTY (M42) 1400 (June 5) with 46's - no tfc (BR)
16218 KRN FAPSI (M42) 1735 (June 6) RTTY/75 msgs 2/1229   (BR)
17464 YBU FAPSI RTTY (M42) 2209 (May 25) with 1/168 msg (BR)
17464 YBU FAPSI (M42) 2207 (June 12)   RTTY (75/425) with "TIKAS" msg:
       "QSL NR 182, NR 183, NR 184" (BR)
17499 //20474 Cherry Ripe E4 2305 (May 24) Sunday Tune barely
       audible; numbers not audible (PFR)
17464 YBU FAPSI (M42) 2207 (June 15)   RTTY (75/425) with "TIKAS" msg
       freq sked for 1400 xmsn. (BR)
18703 YBU FAPSI RTTY (M42) 1408 (June 4) with 1/75 msg (BR)
19889 Cherry Ripe E4 0000 (June 3) usb 03068(CT)
20117 YBU FAPSI RTTY (M42) 2200 (May 25) with 1/168 msg (BR)
20117 YBU FAPSI (M42) 2200 (June 9) RTTY/75 msg 1/123 (BR)
23461 // 17499 // 20474 jammed   Cherry Ripe E4 2300 (June 3) usb
       63696 5ngs.(CT).

++
                      xtra
++
Guy Denman remarks:

Hi All,
I have noticed particularly with Morse Stations, that they are coming
up on the same frequency as 1 year ago in 1997. It does not apply to
all families, but so far I have seen it with M1B, M3,M12, and M13. M3
is even sending the same message as it sent a year ago. It might be
worth checking your logs of voice stations to see if they are doing
the same. I have not heard anything at all of G2 this week. It is one
of those funny weeks, week 5 of May. I will have another listen next
week as that will be week 1 of June.

from Tom Sevart:

Hey gang,
The mystery station P7X is back, this time on 5879.5 with its usual
120 grp 5L msgs interspersed with data xmissions. I logged P7X on
4439.5 a couple weeks ago. I think it may possibly be working

parallel on both freqs, but I don't hear it on 4439.5 at the moment.

++
Contributors:
AB: Ary Boender, Spijkenisse, the Netherlands
Abe: Andrew Bell, Merseyside, UK
ANUS: Anonymous Eastern USA
BR: Bob Roehrig, Aurora, IL
CT: Clarence Thompson, Texas, USA
EB: Eric KC5WCP P.O. Box 896 Biloxi, MS
GD2   Guy Denman, England
HFD: Hans-Friedrich Dumrese, Trier, Germany
JL: Jason Lillie
JM: John Mondary, Annmore, WV, USA
ML: Murray Lehman, Perth, Australia
PFR: Paul F. Reah, Phoenix, AZ
SD: Simon Deneen,Gold Coast, Queensland, Australia.

tnx for all contributions !

000 000 znn de jascha